JOURNAL OF NUMBER THEORY 32, 131–150 (1989)

$\mathbb{Z}_p$-Extensions of Complex Multiplication Fields

INA KERSTEN

FB Mathematik, Gaußstraße 20, D-5600 Wuppertal 1, Federal Republic of Germany

AND

JOHANNES MICHALIČEK

Mathematisches Seminar, Bundesstraße 55, D-2000 Hamburg 13, Federal Republic of Germany

Communicated by H. Zassenhaus

Received November 8, 1987

Suppose, K is a number field, and p is an odd prime. Setting $R_K = \mathfrak{O}_K[p^{-1}]$ with $\mathfrak{O}_K$ being the ring of integers of K, the isomorphism classes of $\mathbb{Z}_p$-extensions of R_K form a $\mathbb{Z}_p$-module $H^1(R_K, \mathbb{Z}_p)$. Leopoldt's conjecture states that $H^1(R_K, \mathbb{Z}_p) \cong \mathbb{Z}_p^{r_2+1}$. In this paper we define a $\mathbb{Z}_p$-submodule $H(R_K, \mathbb{Z}_p)$ of $H^1(R_K, \mathbb{Z}_p)$ consisting of those classes of $\mathbb{Z}_p$-extensions having a normal basis over R_K. We prove for a complex multiplication field K that there is an isomorphism $H(R_K, \mathbb{Z}_p) \cong \mathbb{Z}_p^{r_2+1}$.

INTRODUCTION

It is known that the isomorphism classes of $\mathbb{Z}_p$-extensions over a connected commutative ring R form a $\mathbb{Z}_p$-module $H^1(R, \Gamma)$ where Γ is a topological group isomorphic to the additive group of p-adic integers $\mathbb{Z}_p$. In this paper we define a $\mathbb{Z}_p$-submodule $H(R, \Gamma)$ consisting of those classes of $\mathbb{Z}_p$-extensions which, in some sense, have a normal basis over R. If K is a number field with ring of integers $\mathfrak{O}_K$ then, setting $R_K = \mathfrak{O}_K[p^{-1}]$, one has $H(R_K, \Gamma) \subset H^1(R_K, \Gamma) \cong H^1(K, \Gamma) = H(K, \Gamma)$.

Leopoldt's conjecture states that there is a $\mathbb{Z}_p$-module isomorphism $H^1(R_K, \Gamma) \cong \mathbb{Z}_p^{r_2+1}$, where r_2 denotes the number of complex places of K.

In this paper we prove for a complex multiplication field K that there is a $\mathbb{Z}_p$-module isomorphism $H(R_K, \Gamma) \cong \mathbb{Z}_p^{r_2+1}$, where p is an odd prime.

If K is a complex multiplication field, there is a direct decomposition

$$H^1(R_K, \Gamma) = C(R_K, \Gamma) \oplus N(R_K, \Gamma)$$

0022-314X/89 $3.00

with $C(R_K, \Gamma) = \{R_\infty \mid \bar{R}_\infty = R_\infty\}$ and $N(R_K, \Gamma) = \{R_\infty \mid \bar{R}_\infty = R_\infty^{-1}\}$, where $^-$ denotes complex conjugation. In Section 4 we show

$$\mathbb{Z}_p\text{-rank } N(R_K, \Gamma) = r_2 \qquad \text{and} \qquad \mathbb{Z}_p\text{-rank } C(R_K, \Gamma) = 1 + \delta(K)$$

with $\delta(K)$ being the "defect of Leopoldt's conjecture." We show, that each Γ-exension without normal basis, which lies in $N(R_K, \Gamma)$, yields an ambigious p-ideal class J of p-power order in the cyclotomic Γ-extension of K, satisfying $\bar{J} = J^{-1}$. We prove in 4.7 that the set of those ideal classes is finite, and we then conclude that the $\mathbb{Z}_p$-ranks of $N(R_K, \Gamma)$ and $N(R_K, \Gamma) \cap H(R_K, \Gamma)$ are the same.

In Section 1 we give definitions of the $\mathbb{Z}_p$-modules $H^1(R, \Gamma)$ and $H(R, \Gamma)$ for a connected commutative ring R, and we establish some lemmas.

In Section 2 we show that the cyclotomic $\mathbb{Z}_p$-field extension of a number field K can be viewed as an element of $H(R_K, \Gamma)$, called Z_∞.

In Section 3 we show that, for a totally real field K, the correspondence $\omega \mapsto Z_\infty^\omega$ induces a $\mathbb{Z}_p$-module isomorphism $\mathbb{Z}_p \xrightarrow{\sim} H(R_K, \Gamma)$.

Finally, in Section 4 we prove the existence of a $\mathbb{Z}_p$-module isomorphism $\mathbb{Z}_p^{r_2+1} \xrightarrow{\sim} H(R_K, \Gamma)$ for a complex multiplication field K.

The results of this paper are announced in [11].

1. $\mathbb{Z}_p$-Extensions of a Connected Commutative Ring

In this section we fix notations and establish some lemmas used in the sequel. The results of this section are more or less well known.

Let p be a prime, and let Γ be a topological group isomorphic to the additive group of p-adic integers $\mathbb{Z}_p$. We write Γ multiplicatively and fix a topological generator τ of Γ. Defining

$$\Gamma_n := \Gamma/\Gamma^{p^n} \qquad \text{and} \qquad \tau_n := \tau \bmod \Gamma^{p^n},$$

the group Γ_n is cyclic of order p^n with generator τ_n for each $n \geqslant 0$.

Assume, R is a commutative ring and $E_n(R)$ is the R-algebra of all functions from Γ_n to R under pointwise multiplication and addition. A commutative ring extension R_n of R is called a *Γ_n-extension*, if Γ_n acts on R_n as a group of R-algebra automorphisms, such that the fixed ring $R_n^{\Gamma_n} = \{x \in R_n \mid \tau_n(x) = x\}$ equals R, and the map $h_n: R_n \otimes_R R_n \to E_n(R_n)$, defined by $h_n(x \otimes y)(\tau_n^i) = x\tau_n^i(y)$ for $x, y \in R_n$ and $i = 0, \ldots, p^n - 1$, is bijective [1]. Examples of Γ_n-extensions are the Galois field extensions with Galois group Γ_n. If L is a Γ_n-field extension of a number field K and if L is unramified over K then the ring $\mathfrak{O}_L$ of integers in L is a Γ_n-extension of the ring $\mathfrak{O}_K$ [1, Remark 1.5(d)].

A further example of a Γ_n-extension of R is the R-algebra $E_n(R)$ when Γ_n acts on $E_n(R)$ via $(\sigma f)(\gamma)=f(\sigma^{-1}\gamma)$ for $\sigma, \gamma \in \Gamma_n$ and $f \in E_n(R)$. We call $E_n(R)$ the *trivial Γ_n-extension* of R.

Let R_∞ be a commutative ring extension of R together with an embedding $\Gamma \subseteq \mathrm{Aut}_R(R_\infty)$ such that the fixed ring R_∞^Γ equals R. Setting

$$R_n := R_\infty^{\Gamma^{p^n}} \qquad \text{for} \quad n \geqslant 0,$$

we obtain inclusions

$$R = R_0 \subset R_1 \subset \cdots \subset R_n \subset \cdots \subset R_\infty,$$

and Γ_n acts on R_n as a group of R-algebra automorphisms such that

$$\tau_m(x) = \tau(x) = \tau_n(x)$$

whenever $x \in R_m$ and $m \leqslant n$. We call R_∞ a Γ-extension (or $\mathbb{Z}_p$-extension) if $R_\infty = \bigcup_{n \geqslant 0} R_n$ and if each R_n is a Γ_n-extension of R.

We now assume that the base ring R is connected (i.e., R has no idempotents other than 0 and 1).

The following lemma follows from [9, p. 280].

1.1. LEMMA. *Let $R_\infty = \bigcup_n R_n$ be a Γ-extension of R. If R_n is a nontrivial Γ_n-extension of R for some $n > 0$ then R_{n+1} is a nontrivial $\langle \tau_{n+1}^{p^n} \rangle$-extension of R_n. In particular, R_∞ is connected if and only if R_1 is connected. If R is a field, then R_∞ is a field if and only if R_1 is a field.*

1.2. EXAMPLE. *If $K_\infty = \bigcup_n K_n$ is a Γ-field extension of a number field K_0 then K_∞ is unramified at all primes not lying above $p\mathbb{Z}$* [15, *Prop.* 13.2]. *Thus, letting $R_n = \mathfrak{O}_{K_n}[p^{-1}]$, then $R_\infty = \bigcup_n R_n$ is a connected Γ-extension of R_0.*

Two Γ-extensions $R_\infty = \bigcup_n R_n$ and $R'_\infty = \bigcup_n R'_n$ of R are called *isomorphic*, if there is an R-algebra isomorphism

$$f\colon R_\infty \to R'_\infty \qquad \text{such that } f \circ \tau = \tau \circ f.$$

If f is such an isomorphism, then $f_n = f_{|R_n}\colon R_n \to R'_n$ is a homomorphism of Γ_n-extensions (i.e., a Γ_n-linear R-algebra homomorphism) and hence an isomorphism [1, Theorem 3.4]. Conversely:

1.3. LEMMA. *Suppose $R_\infty = \bigcup_n R_n$ and $R'_\infty = \bigcup_n R'_n$ are two Γ-extensions of R. If there is an isomorphism $R_n \cong R'_n$ of Γ_n-extensions for each $n > 0$, then R_∞ and R'_∞ are isomorphic as Γ-extensions.*

Proof. We have to construct isomorphisms $f_n: R_n \xrightarrow{\sim} R'_n$ such that $f_{n|R_{n-1}} = f_{n-1}$ for all $n > 0$. Let $g_n: R_n \xrightarrow{\sim} R'_n$ be an isomorphism of Γ_n-extensions for all $n > 0$.

If R_∞ is connected and if f_n is constructed, there is a unique $i \in \mathbb{Z}$ such that $f_n = \tau_n^i \circ (g_{n+1|R_n})$ by [1, Cor. 3.2]. Setting $f_{n+1} = \tau_{n+1}^i \circ g_{n+1}$ the result follows.

If R_∞ is nonconnected, then either $R_n \cong E_n(R)$ for all n, or there is $c \in \mathbb{N}$ such that $R_n \cong E_n(R)$ for all $n \leqslant c$ and R_n is a nontrivial $\langle \tau_n^{p^c} \rangle$-extension of R_c for all $n > c$ by Lemma 1.1.

Suppose c exists. Write $R_c = \bigoplus_i Re_i$ with $\{e_i \mid 0 \leqslant i \leqslant p^c - 1\}$ a set of pairwise orthogonal idempotents whose sum is 1, and $\tau_c(e_i) = e_{i+1}$ for all i. Note that since R is connected each idempotent of R_c, hence of R_∞, is a sum of elements e_i. Now $\{g_n(e_0) \mid n \geqslant c\}$ is a finite subset of R'_c. Hence there is an idempotent $v_0 \in R'_c$ such that $v_o = g_n(e_0)$ for infinitely many $n \geqslant c$. Replacing g_n by the restriction of g_{n+1} if necessary, we may assume $v_0 = g_n(e_0)$ for *all* $n \geqslant c$. The Γ-extension $e_0 R_\infty$ of $e_0 R_c \cong R$ is connected, hence there are isomorphisms $f_{n,0}: e_0 R_n \to v_0 R'_n$ with $f_{n,0|R_{n-1}} = f_{n-1,0}$ for all $n > c$. Setting $f_{n,i}(e_i x) = \tau_n^i(f_{n,0}(e_0 \tau_n^{-i}(x)))$ for $x \in R_n$, $i = 0, ..., p^c - 1$, we obtain an isomorphism of Γ_n-extensions $f_n: R_n \xrightarrow{\sim} R'_n$ defined by $f_n(x) = \sum_i f_{n,i}(e_i x)$, such that $f_{n|R_{n-1}} = f_{n-1}$ for all $n > c$, and by restriction for all n.

Finally assume $R_n = E_n(R)$ for all n. Suppose we have constructed $f_n: R_n \xrightarrow{\sim} R'_n$ with $f_{n|R_{n-1}} = f_{n-1}$. Define $e_0 \in E_n(R)$ by $e_0(\tau_n^j) = \delta_{0,j}$ (Kronecker symbol) and set $f_n(e_0) = v_0$. Choose $e_0^{(n+1)} \in E_{n+1}(R)$ and $v_0^{(n+1)} \in E_{n+1}(R')$ with $e_0 = \mathrm{tr}(e_0^{(n+1)})$ and $v_0 = \mathrm{tr}(v_0^{(n+1)})$ where tr denotes the trace map from R_{n+1} (resp. R'_{n+1}) to R_n (resp. R'_n). Then setting $f_{n+1}(\tau_{n+1}^i(e_0^{(n+1)})) = \tau_{n+1}^i(v_0^{(n+1)})$ for $i = 0, ..., p^{n+1} - 1$ we obtain an isomorphism $f_{n+1}: R_{n+1} \xrightarrow{\sim} R'_{n+1}$ of Γ_{n+1}-extensions with $f_{n+1|R_n} = f_n$. ∎

It is known that the isomorphism classes of Γ_n-extensions form a commutative group

$$H^1(R, \Gamma_n) \cong H^1_{et}(R, \Gamma_n)$$

such that $E_n(R)$ represents the unit element [7; 14; 6, 2]. $H^1(R, \Gamma_n)$ has p^n-torsion and hence is a $(\mathbb{Z}/p^n\mathbb{Z})$-module as follows from [7, Theorem 4].

The canonical projection $\Gamma_n \to \Gamma_m$ for $m \leqslant n$ induces a group homomorphism

$$\gamma_{m,n}: H^1(R, \Gamma_n) \to H^1(R, \Gamma_m), \qquad R_n \mapsto R_n^{\langle \tau_n^{p^m} \rangle},$$

such that $\gamma_{j,n} = \gamma_{j,m} \circ \gamma_{m,n}$ for $j \leqslant m \leqslant n$ [1, 14]. We therefore have a $\mathbb{Z}_p$-module $\varprojlim H^1(R, \Gamma)$ with respect to the projective system

$(H^1(R, \Gamma_m), \gamma_{m,n})$. Letting $H^1(R, \Gamma)$ be the set of isomorphism classes of Γ-extensions of R we obtain a map

$$\varphi: H^1(R, \Gamma) \to \varprojlim H^1(R, \Gamma_n), \qquad \bigcup_n R_n = R_\infty \mapsto (R_n)_{n \geqslant 0},$$

being injective because of Lemma 1.3. If $(R_n)_n \in \varprojlim H^1(R, \Gamma_n)$, one constructs an inductive system $\{R_m, \iota_{m,n}: R_m \subsetneq R_n \mid m \leqslant n\}$ starting with embeddings $\iota_{n-1,n}: R_{n-1} \xrightarrow{\sim} R_n^U \subset R_n$ where $U = \langle \tau_n^{p^{n-1}} \rangle$. Hence φ is bijective, and $H^1(R, \Gamma)$ is a $\mathbb{Z}_p$-module via φ.

For each $n > 0$ there is a subgroup $H(R, \Gamma_n)$ of $H^1(R, \Gamma_n)$ consisting of those classes of Γ_n-extensions which have a normal basis over R, and $\gamma_{m,n}$ induces a group homomorphism $H(R, \Gamma_n) \to H(R, \Gamma_m)$ for $m \leqslant n$ [14, 1]. Let $H(R, \Gamma)$ be the subset of $H^1(R, \Gamma)$ consisting of those classes of Γ-extensions $R_\infty = \bigcup_n R_n$ such that each R_n has a normal basis over R. Then $H(R, \Gamma)$ is a $\mathbb{Z}_p$-submodule of $H^1(R, \Gamma)$, since the projective limit is left exact.

Let $E_\infty(R)$ be the R-algebra of all continuous functions $f: \Gamma \to R$ where R is provided with the discrete topology. $E_\infty(R)$ represents the unit element in $H(R, \Gamma)$ when Γ acts on $E_\infty(R)$ via $(\sigma f)(\gamma) = f(\sigma^{-1}\gamma)$ for $\sigma, \gamma \in \Gamma$ and $f \in E_\infty(R)$. Given any Γ-extension $R_\infty = \bigcup_n R_n$ of R the map $h_\infty: R_\infty \otimes_R R_\infty \to E_\infty(R_\infty)$, $h_\infty(x \otimes y)(\gamma) = x\gamma(y)$ for $x, y \in R_\infty$, $\gamma \in \Gamma$, is bijective. If each R_n has a normal basis over R there is a Γ-linear R-module isomorphism $R_\infty \cong E_\infty(R)$; this can be verified with help of [10, Prop. 5.4] and is shown in [13] for infinite Galois field extensions.

The character groups

$$G_n = \hat{\Gamma}_n = \{\sigma \in \mathrm{Hom}_{\mathrm{cont}}(\Gamma, \mathbb{C}^*) \mid \sigma(z) = 1 \ \forall z \in \Gamma^{p^n}\}$$

with $\mathbb{C}^* = \mathbb{C} \setminus 0$ yield inclusions

$$1 = G_0 \subset G_1 \subset \cdots \subset G_n \subset \cdots \subset G_\infty = \mathrm{Hom}_{\mathrm{cont}}(\Gamma, \mathbb{C}^*)$$

and G_n is a cyclic group of order p^n for all n. We choose generators σ_n of G_n such that $\sigma_n^p = \sigma_{n-1}$ for all $n > 0$. Let $R[G_n] = \oplus_{i=0}^{p^n-1} R\sigma_n^i$ be the commutative group ring of G_n with coefficients in R.

Defining for $j \in \mathbb{Z}$ an R-algebra homomorphism

$$v_j: R[G_n] \to R[G_n] \qquad \text{via } v_j(\sigma_n) = \sigma_n^j$$

we have $v_i \circ v_j = v_{ij}$ and $v_j = v_{j \bmod p^n}$ for all $i, j \in \mathbb{Z}$.

Because of the following lemma, proved in [10, Lemma 1.3], we may regard a normal basis of a Γ_n-extension R_n of R as a unit in the group ring $R_n[G_n]$.

1.4. LEMMA. *Let R_n be a Γ_n-extension of R, and let $X=\sum_{i=0}^{p^n-1} X_i\sigma_n^{-i}$ be in $R_n[G_n]$. Then the following conditions are equivalent:*

(i) *$X_0, \ldots, X_{p^n-1}$ is an R-basis of R_n over R and $X_i=\tau_n^i(X_0)$ for all i.*

(ii) *X is a unit in $R_n[G_n]$ and $\tau_n(X)=\sigma_n X$, where τ_n acts on the coefficients of X and $\sigma_n X$ is the product of σ_n with X in $R_n[G_n]$.*

If p is odd it easily follows from 1.4:

1.5. LEMMA. *If Y is a normal basis of a Γ_n-extension R_n of R, then $X=(Yv_{-1}(Y)^{-1})^{(p^n+1)/2}$ is a normal basis of R_n over R satisfying*

$$v_0(X)=1 \qquad \text{and} \qquad X^{-1}=v_{-1}(X). \tag{$*$}$$

We call a normal basis satisfying the equations $(*)$ a *normalized normal basis.*

Since R is connected there is a separable closure R^{sep}. If p is a unit in R then R^{sep} contains a primitive p^nth root of unity ζ_n. Defining for $i\in\mathbb{Z}$ an R-algebra homomorphism

$$\chi_i\colon R[G_n]\to R(\zeta_n) \qquad \text{via } \chi_i(\sigma_n)=\zeta_n^i$$

we have $\chi_i\circ v_j=\chi_{ij}$ for all $i, j\in\mathbb{Z}$.

If $x\in R[G_n]$ then $\chi_i(x)$ is the ith *Fourier coefficient* of x, and the following lemma is easily checked.

1.6. LEMMA. *Let p be a unit in R. If $x=\sum_{i=0}^{p^n-1} x_i\sigma_n^{-i}$ in $R[G_n]$ then $x_i=p^{-n}\sum_{j=0}^{p^n-1}\chi_j(x)\zeta_n^{ij}$ for all $i=0, \ldots, p^n-1$.*

2. A NORMAL BASIS OF THE CYCLOTOMIC $\mathbb{Z}_p$-EXTENSION OF A NUMBER FIELD

Let K_0 be a number field, i.e., a finite field extension of the rationals $\mathbb{Q}$, and let $K_\infty=\bigcup_n K_n$ be the cyclotomic $\mathbb{Z}_p$-field extension of K_0 [15, Sect. 7.3]. For each n we denote by μ_{p^n} the group of the p^nth roots of unity in K^{sep}. Let $n_0\in\mathbb{N}$ be maximal with respect to the property

$$\mu_{p^{n_0}}\subset K(\mu_p).$$

Let $\mathfrak{O}_{K_n}$ be the ring of integers in K_n and set $Z_n=\mathfrak{O}_{K_n}[p^{-1}]$.

2.1. THEOREM. *If p is odd, Z_n has a normalized normal basis $X^{(n)}$ over Z_0 for all $n>0$ such that the Fourier coefficients $\chi_j(X^{(n)})$ are p^{n+n_0}th roots of unity for $j=0, \ldots, p^n-1$.*

Proof. We first prove that $Z_n(\mu_p)$ has a normalized normal basis over $Z_0(\mu_p)$ with Fourier coefficients being p^{n+n_0}th roots of unity. Let

$$M_n := \{m \in \mathbb{Z} \mid -(p^n-1)/2 \leqslant m \leqslant (p^n-1)/2\}$$

for $n \geqslant 0$. Let ζ_{n+n_0} be a primitive p^{n+n_0}th root of unity in $Z_n(\mu_p)$ such that

$$\tau_n(\zeta_{n+n_0}) = \zeta_{n+n_0}^{1+p^{n_0}}.$$

Set $\zeta_n = \zeta_{n+n_0}^{p^{n_0}}$.

Suppose $n \leqslant n_0$. Then define $X_k := p^{-n} \sum_{m \in M_n} \zeta_{n+n_0}^m \zeta_n^{km}$ for $k = 0, \ldots, p^n - 1$. Setting

$$X = X^{(n)} = \sum_{k=0}^{p^n-1} X_k \sigma_n^{-k}$$

we obtain $\chi_j(X) = \zeta_{n+n_0}^j$ and $\chi_j(v_{-1}(X)) = \zeta_{n+n_0}^{-j}$ for $j = 0, \ldots, p^n - 1$. Since $\chi_j(v_0(X)) = \chi_0(X) = 1$ for all j, Lemma 1.6 implies that X is normalized. Since $n \leqslant n_0$ we have $\tau_n(X_k) = X_{k+1}$ for all $k = 0, \ldots, p^n - 1$, hence $\tau_n(X) = \sigma_n X$. Using Lemma 1.4 the assertion follows for $n \leqslant n_0$, and by induction on n we shall prove it for $n \geqslant n_0$.

Assume that $X^{(n)}$ is a normalized normal basis of $Z_n(\mu_p)$ over $Z_0(\mu_p)$ with Fourier coefficients being p^{n+n_0}th roots of unity, and assume $n > n_0$. Let $m \in M_{n+1}$. If p divides m then $m = pr$ for a unique $r \in M_n$ and we define

$$\hat{X}_m^{(n+1)} = \chi_r(X^{(n)}) =: \hat{X}_r^{(n)}.$$

If p does not divide m then $m = i\,(1 + p^{n_0})^{-l}$ for a unique $i \in M_{n_0}$ such that p does not divide i, and a unique $l \in L := \{0, \ldots, p^{n+1-n_0} - 1\}$. We then define

$$\hat{X}_m^{(n+1)} = \zeta_{n+1+n_0}^{i(1+lp^{n_0})(1+p^{n_0})^{-l}}.$$

Setting

$$X^{(n+1)} = \sum_{k=0}^{p^{n+1}-1} X_k^{(n+1)} \sigma_{n+1}^{-k} \qquad \text{with} \quad X_k^{(n+1)} = p^{-(n+1)} \sum_{m \in M_{n+1}} \hat{X}_m^{(n+1)} \zeta_{n+1}^{km}$$

we have $\chi_j(X^{(n+1)}) = \hat{X}_j^{(n+1)}$ for all $j = 0, \ldots, p^{n+1} - 1$ being p^{n+1+n_0}th roots of unity by definition and induction. $X^{(n+1)}$ is normalized by Lemma 1.6 since $\hat{X}_j^{(n+1)} \hat{X}_{-j}^{(n+1)} = 1$ for all j and $\hat{X}_0^{(n+1)} = 1$. It remains to check that $\tau_{n+1}(X_k^{(n+1)}) = X_{k+1}^{(n+1)}$ for $k = 0, \ldots, p^{n+1} - 1$. By induction we have

$$\tau_{n+1}\left(\sum_{\substack{m \in M_{n+1} \\ p \mid m}} \hat{X}_m^{(n+1)} \zeta_{n+1}^{km}\right) = \tau_n\left(\sum_{r \in M_n} \hat{X}_r^{(n)} \zeta_n^{kr}\right) = \sum_r \hat{X}_r^{(n)} \zeta_n^{(k+1)r}$$

$$= \sum_{\substack{m \in M_{n+1} \\ p \mid m}} \hat{X}_m^{(n+1)} \zeta_{n+1}^{(k+1)m}.$$

Finally, we compute

$$\tau_{n+1}\left(\sum_{\substack{m\in M_{n+1}\\(p,m)=1}} \hat{X}_m^{(n+1)}\zeta_{n+1}^{km}\right)=\tau_{n+1}\left(\sum_{i\in M_{n_0}}\sum_{l\in L}\zeta_{n+1+n_0}^{i(1+lp^{n_0})(1+p^{n_0})^{-l}}\zeta_{n+1}^{ki(1+p^{n_0})^{-l}}\right)$$

$$=\sum_i\sum_l \zeta_{n+1+n_0}^{i(1+lp^{n_0})(1+p^{n_0})^{-l+1}+kip^{n_0}(1+p^{n_0})^{-l+1}}$$

$$=\sum_i\sum_l \zeta_{n+1+n_0}^{i(1+(l+1)p^{n_0})(1+p^{n_0})^{-l}+kip^{n_0}(1+p^{n_0})^{-l}}$$

$$=\sum_i\sum_l \zeta_{n+1+n_0}^{i(1+lp^{n_0})(1+p^{n_0})^{-l}+ip^{n_0}(1+p^{n_0})^{-l}+kip^{n_0}(1+p^{n_0})^{-l}}$$

$$=\sum_i\sum_l \zeta_{n+1+n_0}^{i(1+lp^{n_0})(1+p^{n_0})^{-l}}\zeta_{n+1}^{i(k+1)(1+p^{n_0})^{-l}}$$

$$=\sum_{\substack{m\in M_{n+1}\\(p,m)=1}} \hat{X}_m^{(n+1)}\zeta_{n+1}^{(k+1)m}.$$

It follows that $\tau_{n+1}(X_k^{(n+1)})=X_{k+1}^{(n+1)}$ for all $k=0,\ldots,p^{n+1}-1$. Thus $X^{(n)}$ is a normalized normal basis of $Z_n(\mu_p)$ over $Z_0(\mu_p)$ with the desired property for all $n>0$.

Let $\mathbf{G}$ be the Galois group of $Z_n(\mu_p)$ over Z_n. Then $\mathbf{G}$ acts on the group ring $Z_n(\mu_p)[G_n]$ by acting on the coefficients. Let $Y=\mathrm{Norm}_{\mathbf{G}}(X^{(n)})$. Then Lemma 1.4 guarantees that Y is a normalized normal basis of Z_n over Z_0. The Fourier coefficients of Y are p^{n+n_0}th roots of unity, since this holds for $X^{(n)}$. ∎

3. The Group $H(R_K, \Gamma)$ for a Totally Real Field K

Let K be a totally real field; i.e., K is a number field and every embedding $K\subsetneq\mathbb{C}$ is real-valued, hence r_2 is zero for K. Let

$$R=R_0=\mathfrak{O}_K[p^{-1}].$$

We denote by $K_\infty=\bigcup_n K_n$ the cyclotomic $\mathbb{Z}_p$-field extension of $K=K_0$ and set $Z_n=\mathfrak{O}_{K_n}[p^{-1}]$ for all n. Assume that p is odd.

3.1. Theorem. *Let $R_\infty=\bigcup_n R_n$ be a connected Γ-extension of R such that R_n has a normal basis over R for all $n>0$. Then there is an R-algebra isomorphism $R_n\cong Z_n$ for all $n>0$.*

Proof. Assume that there is $n_1>0$ such that R_{n_1} is not isomorphic to Z_{n_1} as an R-algebra.

As in Section 2 let $n_0 \in \mathbb{N}$ be maximal such that $\mu_{p^{n_0}} \subset K(\mu_p)$. Choose an integer m_0 such that every prime ideal of $\mathfrak{O}_{K_{m_0}(\mu_p)}$ lying above $p\mathbb{Z}$ is totally ramified in $K_\infty(\mu_p)$ [8, Sect. 6, Lemma 4]. Choose $n \in \mathbb{N}$ such that

$$n > n_1 + c \qquad \text{with} \quad c = n_0 + m_0.$$

Let $X = \sum_{i=0}^{p^n-1} X_i \sigma_n^{-i} \in R_n[G_n]$ be a normal basis of R_n over R. By 1.5 we may assume that X is normalized. Recall that $v_j(\sigma_n) = \sigma_n^j$ for $j \in \mathbb{Z}$. Let

$$Y := X v_{p^c+1}(X)^{-1}.$$

We think of R_∞ and Z_∞ as sitting in the same separable closure R^{sep} of R. We shall prove that there is an integer s with $(p, s) = 1$ such that

$$Y^s \in Z_{2n}[G_n]. \tag{$*$}$$

From $(*)$ we get a contradiction in the following way: Since R_∞ and Z_∞ are both Γ-extensions there is $m \geqslant 0$ such that $Z_m = Z_{2n} \cap R_n = R_m$, thus $Y^s \in R_m[G_n]$ by $(*)$. This yields $\tau_n^{p^m}(Y^s) = Y^s$, since the Galois group of R_n over R_m is generated by $\tau_n^{p^m}$. On the other hand, Lemma 1.4 implies

$$\tau_n^{p^m}(Y^s) = \tau_n^{p^m}(X v_{p^c+1}(X)^{-1})^s = (\sigma_n^{p^m} \sigma_n^{-p^m(p^c+1)} Y)^s = \sigma_n^{-sp^{m+c}} Y^s.$$

Since Y^s is a unit, it follows that $\sigma_n^{-sp^{m+c}} = 1$. By assumption we have $n_1 > m$, hence $n > n_1 + c > m + c$. Since $(p, s) = 1$ this implies $\sigma_n^{-sp^{m+c}} \neq 1$ and hence a contradiction. Thus Theorem 3.1 follows from $(*)$.

It follows from Lemma 1.4 that $\tau_n(X^{p^n}) = (\sigma_n X)^{p^n} = X^{p^n}$, hence $X^{p^n} \in R[G_n]$ and so $Y^{p^n} \in R[G_n]$. In order to prove $(*)$ it suffices to show that each Fourier coefficient

$$q_j = \chi_j(Y^{p^n}), \qquad j = 0, \ldots, p^n - 1,$$

is a root of unity in R^{sep} for the following reason. We have $q_j \in R(\zeta_n) \subset Z_n(\mu_p)$. If q_j is a root of unity and if the order of q_j is $s_j p^r$ with $r \in \mathbb{Z}$ and $(p, s_j) = 1$ then, setting $s = \prod_{j=0}^{p^n-1} s_j$, we obtain $\chi_j(Y^s) \in Z_{2n}(\mu_p)$ for $j = 0, \ldots, p^n - 1$. Lemma 1.6 then implies $Y^s \in Z_{2n}(\mu_p)[G_n]$. Since $Z_{2n}(\mu_p) \cap R_n \subset Z_{2n}$ we get $Y^s \in Z_{2n}[G_n]$ and hence $(*)$.

If x is an algebraic integer all whose conjugates have absolute value 1 in $\mathbb{C}$, then x is a root of unity [15, Lemma 1.6]. Since $K(\zeta_n)$ is a complex multiplication field it remains to prove $q_j \in \mathcal{O}_{K(\zeta_n)}$ and $|q_j| = q_j \bar{q}_j = 1$, where $\bar{q}_j$ is the complex conjugate of q_j.

Let $\zeta_1 = \zeta_n^{p^{n-1}}$ and $\zeta_c = \zeta_n^{p^{n-c}}$. Then $K(\zeta_n)$ is a Galois field extension of $K(\zeta_1)$ with Galois group $\mathbf{G}$ of order p^{n-n_0}. There is $\rho \in \mathbf{G}$ such that $\rho(x) = x$ for all $x \in K(\zeta_c)$ and

$$\rho(\zeta_n) = \zeta_n^{p^c+1}.$$

Setting $X^{p^n} = T = \sum_{i=0}^{p^n-1} T_i \sigma_n^{-i}$ with $T_i \in R$ we get $T^{-1} = v_{-1}(T) = \sum_i T_i \sigma_n^i$, since X is normalized. This implies $\chi_j(v_{p^c+1}(T)^{-1}) = \rho(\chi_j(T)^{-1}) = \rho(\chi_j(T))^{-1}$ and hence

$$q_j = \chi_j(T)\rho(\chi_j(T))^{-1} \qquad \text{for all } j = 0, \ldots, p^n - 1.$$

Since the coefficients T_i of T are in the totally real field K we have $\chi_j(T)^{-1} = \overline{\chi_j(T)}$ forcing $|\chi_j(T)| = 1$ and $|\rho(\chi_j(T))| = \rho(|\chi_j(T)|) = 1$, thus $|q_j| = 1$ for all $j = 0, \ldots, p^n - 1$.

It remains to show that q_j is an algebraic integer. Let

$$\chi_j(T)\mathfrak{O}_{K(\zeta_n)} = \prod_{\mathfrak{p}} \mathfrak{p}^{\alpha(\mathfrak{p})}$$

with $\alpha(\mathfrak{p}) \in \mathbb{Z}$ and $\alpha(\mathfrak{p}) = 0$ for almost all $\mathfrak{p}$ be the prime ideal decomposition of the fractional ideal $\chi_j(T)\mathfrak{O}_{K(\zeta_n)}$. If $\alpha(\mathfrak{p})$ is nonzero then $\mathfrak{p}$ lies above $p\mathbb{Z}$ since $\chi_j(T)$ is a unit in $R(\zeta_n)$. We therefore have $\rho(\mathfrak{p}) = \mathfrak{p}$ since there is only one prime ideal above $\mathfrak{p} \cap \mathfrak{O}_{K(\zeta_c)}$ by definition of m_0 and $n > c$. It follows that $q_j \mathfrak{O}_{K(\zeta_n)} = \prod_{\mathfrak{p}} \mathfrak{p}^{\alpha(\mathfrak{p})} \prod_{\mathfrak{p}} \mathfrak{p}^{-\alpha(\mathfrak{p})} = \mathfrak{O}_{K(\zeta_n)}$ forcing that q_j is an algebraic integer for $j \in \{0, \ldots, p^n - 1\}$. ∎

3.2. COROLLARY. *Let $R_\infty = \bigcup_n R_n$ be a nontrivial Γ-extension of R such that R_n has a normal basis for all n; then there is an isomorphism of Γ-extensions $R_\infty \cong Z_\infty^\omega$ for some $\omega \in \mathbb{Z}_p$.*

Proof. We first consider the case that R_∞ is connected. By Theorem 3.1 there is an R-algebra isomorphism $f_n : R_n \xrightarrow{\sim} Z_n$ for all $n > 0$. Letting $\gamma_n : Z_n \to Z_n$, $x \mapsto (f_n \circ \tau_n \circ f_n^{-1})(x)$, then $\gamma_n(f_n(x)) = f_n(\tau_n(x))$ for all $x \in R_n$. Since Γ_n is isomorphic to the group of all R-algebra automorphisms of Z_n, it follows that there is $j_n \in \mathbb{Z}$ with $(j_n, p) = 1$ and $\gamma_n = \tau_n^{j_n}$. Let $Z_n(j_n)$ be the R-algebra Z_n endowed with Γ_n-action $\Gamma_n \times Z_n(j_n) \to Z_n(j_n)$, $(\tau_n, x) \mapsto \tau_n^{j_n}(x)$. Choose $i_n \in \mathbb{Z}$ with $i_n j_n \equiv 1 \bmod p^n\mathbb{Z}$. Then $[R_n] = [Z_n(j_n)] = [Z_n]^{i_n}$ in $H(R, \Gamma_n)$ as follows from [7, Theorem 4]. Since p^m is the order of $[Z_m]$ we have $i_n \equiv i_m \bmod p^m\mathbb{Z}$ for all $m \leqslant n$. Thus there is $i \in \mathbb{Z}_p$ with $i_n = i \bmod p^n\mathbb{Z}_p$ for all n, and we have an isomorphism $R_\infty \cong Z_\infty^i$ of Γ-extensions by 1.3.

If R_∞ is nonconnected, but nontrivial then $S_\infty := R_\infty Z_\infty$ is connected by 1.1 and since $\varphi : H^1(R, \Gamma) \to \varprojlim H^1(R, \Gamma_n)$, defined in Section 1, is an isomorphism of groups. As we have shown there is a unit i in $\mathbb{Z}_p$ and an isomorphism $S_\infty \cong Z_\infty^i$ of Γ-extensions. We therefore have $R_\infty \cong Z_\infty^i Z_\infty^{-1} \cong Z_\infty^\omega$ with $\omega = i - 1$. ∎

3.3. COROLLARY. *There is a $\mathbb{Z}_p$-module isomorphism $\mathbb{Z}_p \xrightarrow{\sim} H(R, \Gamma)$, $\omega \mapsto Z_\infty^\omega$.*

Proof. By Theorem 2.1 we have $[Z_\infty]^\omega \in H(R, \Gamma)$, and by 3.2 the map $\mathbb{Z}_p \to H(R, \Gamma)$, $\omega \mapsto Z_\infty^\omega$, is surjective. It is injective, since $(Z_n^{p^k})^l$ with $k, l \in \mathbb{Z}$ and $(p, l) = 1$ is not trivial for $n > k$. ∎

Remark. It is proved in [5] that $|H(R_K, \Gamma_n)| = p^{n(r_2+1)} \cdot O(1)$ for an arbitrary number field K. This result combined with Theorem 2.1 also implies that there is a $\mathbb{Z}_p$-module isomorphism $H(R_K, \Gamma) \cong \mathbb{Z}_p$ for a totally real field K.

4. The Group $H(R_K, \Gamma)$ for a CM-Field K

Let K be a complex multiplication field, i.e., K is a totally imaginary quadratic field extension of a totally real field, denoted by K^+. The Galois group of K over K^+ is generated by an automorphism ι which for each embedding $K \subsetneq \mathbb{C}$ coincides with complex conjugation. Write $\iota(\lambda) = \bar{\lambda}$ for $\lambda \in K$. Assume that p is an odd prime, and set

$$R = \mathfrak{O}_K[p^{-1}] \qquad \text{and} \qquad R^+ = \mathfrak{O}_{K^+}[p^{-1}].$$

For any R-module M define the R-module $\bar{M}$ to be the additive group M equipped with a new R-structure $\lambda \cdot x = \bar{\lambda} x$ for $\lambda \in R$ and $x \in M$.

We define in $H^1(R, \Gamma)$ two $\mathbb{Z}_p$-submodules

$$C(R, \Gamma) = \{R_\infty \in H^1(R, \Gamma) \mid \bar{R}_\infty = R_\infty\} \qquad \text{and}$$
$$N(R, \Gamma) = \{R_\infty \in H^1(R, \Gamma) \mid \bar{R}_\infty = R_\infty^{-1}\}.$$

Since $R_\infty = (R_\infty \cdot \bar{R}_\infty)^{1/2} \cdot (R_\infty \cdot \bar{R}_\infty^{-1})^{1/2}$ for each $R_\infty \in H^1(R, \Gamma)$, one has

$$H^1(R, \Gamma) = C(R, \Gamma) \oplus N(R, \Gamma).$$

It is known that there is a $\mathbb{Z}_p$-module isomorphism $H^1(R, \Gamma) \cong \mathbb{Z}_p^{r_2+1+\delta}$ for some $\delta = \delta(K) \geqslant 0$, where r_2 denotes the number of complex places of K. The conjecture $\delta(K) = 0$ is called *Leopoldt's conjecture* [15, Sect. 5.5 and Theorem 13.4].

In this section we first compute the $\mathbb{Z}_p$-ranks of $C(R, \Gamma)$ and $N(R, \Gamma)$:

$$\mathbb{Z}_p\text{-rank } N(R, \Gamma) = r_2 \qquad \text{and} \qquad \mathbb{Z}_p\text{-rank } C(R, \Gamma) = 1 + \delta(K^+).$$

We then prove, that the $\mathbb{Z}_p$-ranks of $N(R, \Gamma)$ and $N(R, \Gamma) \cap H(R, \Gamma)$ are the same, and this yields the existence of a $\mathbb{Z}_p$-module isomorphism

$$H(R, \Gamma) \cong \mathbb{Z}_p^{r_2+1}.$$

4.1. Proposition. (a) *There is a $\mathbb{Z}_p$-module isomorphism $H^1(R^+, \Gamma) \xrightarrow{\sim} C(R, \Gamma)$ given by $R_\infty^+ \mapsto R_\infty^+ \otimes_{R^+} R$.*

(b) *Suppose* $R_\infty = \bigcup_n R_n$ *is a connected* Γ*-extension of* R*, and* K_n *is the quotient field of* R_n*. If* R_∞ *lies in* $C(R, \Gamma)$ *then each* K_n *is a complex multiplication field.*

Proof. The canonical homomorphism $H^1(R^+, \Gamma_n) \to H^1(R, \Gamma_n)$ is injective and induces an injective $\mathbb{Z}_p$-module homomophism $\varphi: H^1(R^+, \Gamma) \to C(R, \Gamma)$. We are going to show that φ is surjective. Assume $R_\infty = \bigcup_n R_n$ is a connected Γ-extension of $R = R_0$ and there is an isomorphism of Γ_n-extensions $f_n: R_n \to \bar{R}_n$ for all n. Then there is a Γ_n-linear ring isomorphism

$$f_n: R_n \to R_n \qquad \text{with} \quad f_n(\lambda x) = \bar{\lambda} f_n(x) \qquad \text{for all } \lambda \in R, \quad x \in R_n.$$

Since R_n is connected the group Γ_n is the group of all R-automorphisms of R_n, hence $f_n^2 = \gamma_n$ for some $\gamma_n \in \Gamma_n$. Setting $s_n = \gamma_n^{-(p^n+1)/2}$ and $\iota_n = s_n f_n$ we obtain $\iota_n(\lambda) = \bar{\lambda}$ for all $\lambda \in R$. Since f_n is Γ_n-linear, we have $\iota_n^2 = id$ and $\iota_n(\tau_n(x)) = \tau_n(\iota_n(x)) = \tau_n(x)$ for all $x \in R_n^+ := R_n^{\langle 1, \iota_n \rangle}$. Thus the group $\Gamma_n = \langle \tau_n \rangle$ acts on R_n^+ as an R^+-automorphism group, and R_n^+ is a Γ_n-extension of R^+ satisfying $R_n^+ \otimes_{R^+} R \cong R_n$. Passing to the quotient fields we obtain $K_n^+ \otimes_{K^+} K \cong K_n$. Since K is a complex multiplication field this yields (b).

We also obtain a Γ-extension $R_\infty^+ = \bigcup_n R_n^+$ of R^+ with $R_\infty^+ \otimes_{R^+} R \cong R_\infty$. Since $C(R, \Gamma)$ is generated by connected Γ-extensions, φ is surjective, and (a) follows. ∎

4.2. COROLLARY. *The* $\mathbb{Z}_p$*-rank of* $C(R, \Gamma)$ *is* $1 + \delta(K^+)$*, and the* $\mathbb{Z}_p$*-rank of* $N(R, \Gamma)$ *is* r_2.

Proof. By 4.1(a), we have $\mathbb{Z}_p$-rank $C(R, \Gamma) = 1 + \delta(K^+)$. Let $E = E(K)$ be the group of units in $\mathfrak{O}_K$. Then the index $(E(K): E(K^+))$ is finite by [15, Th. 4.12]. With the notations of [15, p. 265] it follows that the index $(E_1(K): E_1(K^+))$ is finite. Thus the index $(\overline{E_1(K)}: \overline{E_1(K^+)})$ is finite too, since the canonical embedding $\overline{E_1(K^+)} \subsetneq \overline{E_1(K)}$ is continuous. This implies $\mathbb{Z}_p$-rank $\overline{E_1(K^+)} = \mathbb{Z}_p$-rank $\overline{E_1(K)}$, hence $\delta(K) = \delta(K^+)$ by [15, p. 265]. We now obtain $\mathbb{Z}_p$-rank $N(R, \Gamma) = \mathbb{Z}_p$-rank $H^1(R, \Gamma) - \mathbb{Z}_p$-rank $C(R, \Gamma) = r_2$. ∎

4.3. COROLLARY. *Leopoldt's conjecture holds for* K *if and only if the cyclotomic* Γ*-field extension is the only* Γ*-extension* $K_\infty = \bigcup_n K_n$ *of* K *such that each* K_n *is a complex multiplication field.*

Proof. Let $K_\infty = \bigcup_n K_n$ be a Γ-field extension of K such that each K_n is a complex multiplication field. If Leopoldt's conjecture is true for K then $\delta(K) = 0 = \delta(K^+)$, hence K_∞ is the cyclotomic $\mathbb{Z}_p$-extension of K. Conversely, if K_∞ is the only Γ-extension of K such that each K_n is a complex mul-

tiplication field, then K_∞ is cyclotomic, and $\mathbb{Z}_p$-rank $C(R, \Gamma) = 1$ by 4.1(b), since $C(R, \Gamma)$ is generated by connected Γ-extensions. Thus 4.2 implies $\mathbb{Z}_p$-rank $H^1(R, \Gamma) = \mathbb{Z}_p$-rank $N(R, \Gamma) + \mathbb{Z}_p$-rank $C(R, \Gamma) = r_2 + 1$. ∎

Given two Γ_n-extensions R_n, R'_n of $R = \mathfrak{O}_K[p^{-1}]$ their product $R_n \cdot R'_n$ is defined to be the Γ_n-extension $(R_n \otimes_R R'_n)^{\ker(\mu)}$ with μ being the multiplication map $\Gamma_n \times \Gamma_n \to \Gamma_n$. This product induces the group structure in $H^1(R, \Gamma_n)$. In particular, R_n^i denotes a representative of the isomorphism class $[R_n]^i \in H^1(R, \Gamma_n)$ for $i \in \mathbb{Z}$.

4.4. THEOREM. *Let $R_\infty = \bigcup_n R_n$ be a Γ-extension of R. If $R_n \cdot \bar{R}_n$ has a normal basis over R for all n there is $s \geqslant 0$, independent of n, such that $R_n^{p^s}$ has a normal basis over R for all n.*

Before proving Theorem 4.4 we show that Theorem 4.4 yields the following corollary.

4.5. COROLLARY. *There is a $\mathbb{Z}_p$-module isomorphism $\mathbb{Z}_p^{r_2+1} \cong H(R, \Gamma)$.*

Proof. Let Z_∞ be the cyclotomic Γ-extension of R and Z_∞^+ the cyclotomic Γ-extension of R^+. It follows from 3.3 that $H(R^+, \Gamma) = \langle Z_\infty^+ \rangle$, thus $H(R, \Gamma) \subset \langle Z_\infty \rangle \oplus N(R, \Gamma)$ by 4.2. Theorems 4.4 and 2.1 imply that there is $t \geqslant 0$ such that $\langle Z_\infty \rangle \oplus N(R, \Gamma)^{p^t} \subset H(R, \Gamma)$. Corollary 4.2 therefore yields $\mathbb{Z}_p$-rank $H(R, \Gamma) = r_2 + 1$. ∎

The rest of this paper is devoted to the proof of Theorem 4.4.

4.6. LEMMA. *Let $\mathfrak{U}$ be the p-Sylow subgroup of the ideal class group of R, and let $\mathfrak{U}^+$ be the p-Sylow subgroup of the ideal class group of R^+. If J denotes the Galois group of K over K^+, the canonical homomorphism $\varphi: \mathfrak{U}^+ \to \mathfrak{U}^J$ is bijective.*

Proof. Let A be an ideal in R^+ such that A^{p^m} is a principal ideal for some m. Suppose $AR = (\alpha)$ for some $\alpha \in R$. Since $\alpha\bar{\alpha} \in R^+$ and $A^2R = (\alpha\bar{\alpha})$, unique factorization into primes implies $A^2 = (\alpha\bar{\alpha})$ in R^+. Thus φ is injective. Let $\mathfrak{C}$ (resp. $\mathfrak{C}^+$) be the p-Sylow subgroup of the ideal class group of $\mathfrak{O}_K$ (resp. $\mathfrak{O}_{K^+}$). Then $|\mathfrak{C}^J| = |\mathfrak{C}^+|$ by [12, Lemma 4.1, p. 64], since $p \neq 2$. Thus the canonical homomorphism $\mathfrak{C}^+ \to \mathfrak{C}^J$ is bijective, and hence φ is surjective. Lemma 4.2 also follows from [8, Lemma 23]. ∎

Viewing a Γ_n-extension of R as a module over the group ring $R[\Gamma_n]$ yields a homomorphism α from $H^1(R, \Gamma_n)$ to $\mathrm{Pic}(R[\Gamma_n])$, the group of isomorphism classes of rank-one projective $R[\Gamma_n]$-modules, and the sequence

$$1 \to H(R, \Gamma_n) \to H^1(R, \Gamma_n) \xrightarrow{\alpha} \mathrm{Pic}(R[\Gamma_n])$$

is an exact sequence of groups [4, Theorem 2]. Any ring homomorphism $f: S \to S'$ induces a homomorphism from $\mathrm{Pic}(S)$ to $\mathrm{Pic}(S')$ denoted by f^*.

Since R is a Dedekind domain we may identify $\mathrm{Pic}(R)$ with the ideal class group of R.

Let μ_{p^n} be the group of p^nth roots of unity in a fixed separable closure of K.

The idea of the proof of 4.4 is the following: Given a Γ-extension $R_\infty = \bigcup_n R_n$ of R with $R_n \cdot \bar{R}_n$ having a normal basis over R, we construct a special sequence $I_n \in \bigcup_{k=0}^{n} \mathrm{Pic}(R(\mu_{p^k}))$, $n \geqslant 0$, such that each I_n has the same order as $\alpha(R_n)$. We then show in Proposition 4.8 below that there is $s \geqslant 0$ with $I_n^{p^s} = 1$ for all n.

As before, let n_0 be maximal such that $\mu_{p^{n_0}}$ lies in $K(\mu_p)$. Then $K_\infty = \bigcup_n K_n$ with $K(\mu_{p^{n+n_0}})$ is the cyclotomic $\mathbb{Z}_p$-extension of $K_0 = K(\mu_p)$, and each K_n is a complex multiplication field. Set

$$Z_n = \mathfrak{O}_{K_n}[p^{-1}] \qquad \text{and} \qquad Z_n^+ = \mathfrak{O}_{K_n^+}[p^{-1}]$$

for all $n \geqslant 0$ and $p \neq 2$. Let $\Gamma_n = \langle \tau_n \rangle$ be the Galois group of K_n over K_0.

4.7. LEMMA. *Let $\mathfrak{U}_n$ be the p-Sylow subgroup of $\mathrm{Pic}(Z_n)$, and let $\mathfrak{B}_n = \{J_n \in \mathfrak{U}_n \mid \tau_n^*(J_n) = J_n$ and $J_n \cdot \bar{J}_n = 1\}$. Then there is an integer $s \geqslant 0$, independent of n, such that $|\mathfrak{B}_n| \leqslant p^s$ for all $n \geqslant 0$.*

Proof. Let $J_n \in \mathfrak{B}_n$. Then $J_n \in \mathfrak{U}_n^{\Gamma_n}$ and $J_n \notin \mathfrak{U}_n^J$ where J is the Galois group of K_n over K_n^+. Choose an integer m_0 such that every prime ideal in $\mathfrak{O}_{K_{m_0}}$ lying above $p\mathbb{Z}$ is totally ramified in K_∞ [8, Sect. 6, Lemma 4]. Set $C_n = \mathfrak{J}_n / P_n$, where $\mathfrak{J}_n$ is the group of all fractional ideals of Z_n and P_n is the subgroup of all principal fractional ideals. We are going to prove $|\mathfrak{B}_n| \leqslant |C_{m_0}|$, and this will prove the lemma.

Let $n > m_0$, and define $G = \Gamma_n^{p^{m_0}}$. The exact sequence

$$0 \to P_n \to \mathfrak{J}_n \to C_n \to 0$$

of G-modules induces an exact sequence

$$0 \to P_n^G \to \mathfrak{J}_n^G \to C_n^G \to H^1(G, P_n) \to 0,$$

since $H^1(G, \mathfrak{J}_n) = 0$ by [12, p. 64]. Thus $|C_n^G| = (\mathfrak{J}_n^G : P_n^G) \cdot |H^1(G, P_n)|$. Since K_n is unramified at all primes not lying above $p\mathbb{Z}$, the canonical homomorphism $\mathfrak{J}_{m_0} \to \mathfrak{J}_n^G$ is bijective and induces a surjective homomorphism $C_{m_0} \to \mathfrak{J}_n^G / P_n^G$, hence $(\mathfrak{J}_n^G : P_n^G) \leqslant |C_{m_0}|$ and $|C_n^G| \leqslant |C_{m_0}| \cdot |H^1(G, P_n)|$.

Let C_n^+ be the ideal class group of Z_n^+. Then $|C_n^{+G}| \geqslant |H^1(G, P_n^+)|$. We therefore obtain $|C_n^G| / |C_n^{+G}| \leqslant |C_{m_0}| \cdot h_1$ with $h_1 = |H^1(G, P_n)| / |H^1(G, P_n^+)|$.

Recall, that $\mathfrak{U}_n$ is the p-Sylow subgroup of C_n. Since $J_n \in \mathfrak{U}_n^G$ and $J_n \notin \mathfrak{U}_n^J$ for all $J_n \in \mathfrak{B}_n$, and since $\mathfrak{U}_n^J \cong \mathfrak{U}_n^+$ by 4.6, we obtain

$$|\mathfrak{B}_n| \leqslant |C_{m_0}| \cdot h_1.$$

It remains to show $h_1 = 1$.

By the choice of m_0 we have $\sigma(\mathfrak{p}) = \mathfrak{p}$ for all $\sigma \in G$ and all prime ideals $\mathfrak{p}$ in $\mathfrak{O}_{K_n}$ lying above $p\mathbb{Z}$. Hence $P_{K_n} = P_n \oplus P_n^{(p)}$ as G-modules, where P_{K_n} is the group of all principal fractional ideals of $\mathfrak{O}_{K_n}$ and $P_n^{(p)}$ is the group of principal fractional ideals of $\mathfrak{O}_{K_n}$ lying over p. Since G acts trivially on $P_n^{(p)}$ and $P_n^{(p)}$ is free, $H^1(G, P_n^{(p)}) = 0$ so

$$H^1(G, P_n) = H^1(G, P_{K_n}).$$

Let E_n be the group of units in $\mathfrak{O}_{K_n}$, and let μ be the group of all roots of unity in K_n. We then have

$$\begin{aligned} |H^1(G, P_n)| &= |(N_G(K_n) \cap E_{m_0})/N_G(E_n)| && \text{by [12, p. 66]} \\ &\leqslant 2\,|(N_G(K_n) \cap \mu E_{m_0}^+)/N_G(\mu E_n^+)| && \text{by [15, Th. 4.12]} \\ &= 2\,|(N_G(K_n) \cap E_{m_0}^+)/N_G(E_n^+)|, \end{aligned}$$

since each root of unity is the norm of a root of unity. Suppose, $x \in N_G(K_n) \cap E_{m_0}^+$, and write $x = N_G(y)$ with $y \in K_n$. Then, setting $z = x^{-1}(y\bar{y})^{(|G|+1)/2}$, we obtain $z \in K_n^+$ and $N_G(z) = x$, hence $N_G(K_n) \cap E_{m_0}^+ = N_G(K_n^+) \cap E_{m_0}^+$. By [12, p. 66], $|(N_G(K_n^+) \cap E_{m_0}^+)/N_G(E_n^+)| = |H^1(G, P_n^+)|$, so we have proved $h_1 \leqslant 2$. Since $x^{|G|} \in N_G(E_n^+)$ for all $x \in N_G(K_n^+) \cap E_{m_0}^+$ the group $H^1(G, P_n^+)$ is a p-group by [12, p. 66], and similarly, $H^1(G, P_n)$ is a p-group. This now yields $h_1 = 1$. ∎

4.8. PROPOSITION. *Assume* $K_\infty = \bigcup_{n \geqslant 0} K_n$ *with* $K_n = K(\mu_{p^{n+n_0}})$, *and* $Z_n = \mathfrak{O}_{K_n}[p^{-1}]$. *Let* $\mathfrak{U}_n$ *be the p-Sylow subgroup of* $\mathrm{Pic}(Z_n)$. *Define* $\rho \in \mathrm{Gal}(K_\infty/K_0)$ *via* $\rho(\zeta) = \zeta^{p^{n_0}+1}$ *for all p-power roots of unity* ζ. *Then there is* $s \geqslant 0$ *such that every* $I \in \bigcup_{k \geqslant 0} \mathfrak{U}_k$, *which satisfies* $I = \bar{I}$ *and* $\rho^*(I) = I^{p^{n_0}+1}$, *satisfies* $I^{p^s} = 1$. *The integer s is independent of I.*

Proof. Define $\mathfrak{B}' = \{I \in \bigcup_{k \geqslant 0} \mathfrak{U}_k \mid I = \bar{I} \text{ and } \rho^*(I) = I^{p^{n_0}+1}\}$.

Suppose, for each $s \geqslant 0$ there is $I(s) \in \mathfrak{B}'$ such that $I(s)^{p^s} \neq 1$. We have $I(s) \in \mathfrak{U}_{k(s)}$ for some $k(s) \geqslant 0$. Since $\mathfrak{U}_{k(s)}$ is a finite group, $k(s)$ cannot be constant, independent of s. So we may assume that there is a sequence $I_n \in \mathfrak{U}_n \cap \mathfrak{B}'$, $n \in \mathbb{N}$, such that for each $s \geqslant 0$ there is $m = m(s)$ with $I_m^{p^s} \neq 1$.

Let $\rho^+ \in \mathrm{Gal}(K_n^+/K_0^+)$ be the image of ρ under the canonical isomorphism $\mathrm{Gal}(K_n/K_0) \cong \mathrm{Gal}(K_n^+/K_0^+)$. Since $I_n = \bar{I}_n$, Lemma 4.6 implies that there is $I_n^+ \in \mathfrak{U}_n^+$ satisfying

$$\rho^{+*}(I_n^+) = (I_n^+)^{p^{n_0}+1} \qquad \text{and} \qquad (I_{m(s)}^+)^{p^s} \neq 1 \qquad \text{for all } s \geqslant 0. \qquad (*)$$

We denote both Galois groups $\mathrm{Gal}(K_n^+/K_0^+)$ and $\mathrm{Gal}(K_n/K_0)$ by the same letter Γ_n.

Let L_n^+ be the maximal abelian, unramified p-extension of K_n^+ in which every prime of K_n^+ lying above $p\mathbb{Z}$ is completely decomposed. L_n^+ is a Galois extension of K_0^+ by the maximality of L_n^+ and the Γ_n-invariance of the set of all prime ideals of K_n^+ lying over p. The Galois group $\Gamma_n = \mathrm{Gal}(K_n^+/K_0^+)$ acts on the Galois group $\mathrm{Gal}(L_n^+/K_n^+)$: let $\tau \in \Gamma_n$; extend to $\tilde{\tau} \in \mathrm{Gal}(L_n^+/K_0^+)$ and set $\sigma^\tau = \tilde{\tau}\sigma\tilde{\tau}^{-1}$ for all $\sigma \in \mathrm{Gal}(L_n^+/K_n^+)$.

The group Γ_n also acts on $\mathfrak{U}_n^+$, the p-Sylow subgroup of $\mathrm{Pic}(Z_n^+)$. The isomorphism of class field theory $\mathfrak{U}_n^+ \xrightarrow{\sim} \mathrm{Gal}(L_n^+/K_n^+)$, induced by the Artin map, is an isomorphism of Γ_n-modules [8, p. 261; 15, p. 339]. Now it follows from $(*)$ that there is a sequence $g_n \in \mathrm{Gal}(L_n^+/K_n^+)$ such that

$$g_n^{\rho^+} = g_n^{p^{n_0}+1} \qquad \text{and} \qquad g_{m(s)}^{p^s} \neq 1 \qquad \text{for all } s \geqslant 0. \tag{$\dagger$}$$

From $(\dagger)$ we get the following

ASSERTION 1. *The field L_n^+ contains an extension D_n^+ of K_n^+ whose Galois group is a Γ_n-module such that $\sigma^{\rho^+} = \sigma^{p^{n_0}+1}$ and $\sigma^{p^n} = 1$ for all $\sigma \in \mathrm{Gal}(D_n^+/K_n^+)$. Furthermore, for each $s \geqslant 0$ there is $m = m(s)$ with $|\mathrm{Gal}(D_m^+/K_m^+)| \geqslant p^s$, and D_n^+ is a Galois extension of K_0^+.*

Proof of Assertion 1. Let $V_n = \mathrm{Gal}(L_n^+/K_n^+)$. Consider the homomorphism $\alpha_n: V_n \to V_n$, $v \mapsto v^{p^{n_0}+1}(v^{\rho^+})^{-1}$ and set $W_n = \alpha_n(V_n)$. Letting D_n^+ be the fixed field of $W_n \cdot V_n^{p^n}$ in L_n^+, it is easily checked that Assertion 1 follows from the definition of W_n and from $(\dagger)$.

We are going to prove that Assertion 1 implies the following

ASSERTION 2. *Let $\mathfrak{B}_n$ be defined as in Lemma* 4.7. *There is a sequence of subgroups $\mathfrak{D}_n$ in $\mathfrak{B}_n$, $n \in \mathbb{N}$, with the property: For each $s \geqslant 0$ there is $m = m(s)$ with $|\mathfrak{D}_m| \geqslant p^s$.*

Since Assertion 2 contradicts Lemma 4.7, the proof of Assertion 2 will finish the proof of Proposition 4.8.

Proof of Assertion 2. Let $D_n = D_n^+(\mu_p)$, where D_n^+ is defined as in Assertion 1. Then $(D_n : D_n^+) = 2$, and D_n is a complex multiplication field. The Galois group G_n of D_n over $K_n = K_n^+(\mu_p)$ is of exponent dividing p_n by Assertion 1. Let $\hat{G}_n = \mathrm{Hom}(G_n, Z_n^*)$, where Z_n^* denotes the units of Z_n. Then $\hat{G}_n \cong G_n$ since Z_n is connected. Since D_n is unramified over K_n the ring $A_n := \mathfrak{O}_{D_n}[p^{-1}]$ is a Galois ring extension of Z_n with Galois group G_n [1, Remark 1.5(d)]. For each $\chi \in \hat{G}_n$ the set

$$I_{n,\chi} = \{a \in A_n \mid \sigma(a) = \chi(\sigma)a \forall \sigma \in G_n\}$$

is a rank-one projective Z_n-module satisfying $I_{n,\chi} \cdot I_{n,\psi}$ for $\chi, \psi \in \hat{G}_n$ by [2, Theorem 1]. Therefore, $\mathfrak{J}_n = \{I_{n,\chi} \mid \chi \in \hat{G}_n\}$ is a group of order $|G_n|$.

Let ρ be defined as in 4.8 and $\rho^*(I_{n,\chi}) = I_{n,\chi} \otimes_{Z_n} \rho_*(Z_n)$, where $\rho_*(Z_n)$ is Z_n considered as a (Z_n)-module via ρ. We are going to show $\bar{I}_{n,\chi} = I_{n,\chi}^{-1}$ and $\rho^*(I_{n,\chi}) \cong I_{n,\chi}$ for all $\chi \in \hat{G}_n$. Since D_n is a complex multiplication field and since $\chi(\sigma)$ is a root of unity, we have

$$\begin{aligned}\overline{I_{n,\chi}} &= \{a \in A_n \mid \sigma(\bar{a}) = \chi(\sigma)\bar{a} \forall \sigma \in G_n\} = \{a \in A_n \mid \overline{\sigma(\bar{a})} = \overline{\chi(\sigma)\bar{a}}\ \forall \sigma \in G_n\} \\ &= \{a \in A_n \mid \sigma(a) = \chi(\sigma)^{-1} a \forall \sigma \in G_n\} = I_{n,\chi^{-1}} = I_{n,\chi}^{-1}.\end{aligned}$$

By Assertion 1 there is an extension $\tilde{\rho} \in \mathrm{Gal}(D_n/K_0)$ of ρ satisfying $\tilde{\rho}\sigma\tilde{\rho}^{-1} = \sigma^{p^{n_0}+1}$ for all $\sigma \in G_n$. The map $\tilde{\rho}(I_{n,\chi}) \to \rho^*(I_{n,\chi})$, $a \mapsto \tilde{\rho}^{-1}(a) \otimes 1$, is a Z_n-module isomorphism with inverse defined by $a \otimes z \mapsto \tilde{\rho}(a)z$ for $a \in I_{n,\chi}$, $z \in Z_n$. We therefore obtain

$$\begin{aligned}\rho^*(I_{n,\chi}) &\cong \{a \in A_n \mid \sigma(\tilde{\rho}^{-1}(a)) = \chi(\sigma)\tilde{\rho}^{-1}(a) \forall \sigma \in G_n\} \\ &= \{a \in A_n \mid (\tilde{\rho}\sigma\tilde{\rho}^{-1})(a) = \tilde{\rho}(\chi(\sigma))a \forall \sigma \in G_n\} \\ &= \{a \in A_n \mid \sigma^{p^{n_0}+1}(a) = \chi(\sigma)^{p^{n_0}+1} a \forall \sigma \in G_n\} = I_{n,\chi}.\end{aligned}$$

We now consider the group homomorphism

$$\beta_n : \mathfrak{J}_n \to \mathrm{Pic}(Z_n), \qquad I_{n,\chi} \mapsto [I_{n,\chi}],$$

where $[I_{n,\chi}]$ denotes the isomorphism class of $I_{n,\chi}$. We have shown that $\mathfrak{D}_n := \beta_n(\mathfrak{J}_n)$ is a subgroup of $\mathfrak{B}_n$. Since $|\mathfrak{J}_n| = |G_n|$ for all n, there is $m = m(s)$ with $|\mathfrak{J}_m| \geqslant p^s$ for each $s \geqslant 0$ by Assertion 1. Showing that there is $r \geqslant 0$, r independent of n, with $|\ker(\beta_n)| \leqslant p^r$ for all n, will thus prove Assertion 2.

Choose an integer m_0 such hat every prime ideal in $\mathfrak{O}_{K_{m_0}}$ lying above $p\mathbb{Z}$ is totally ramified in K_∞ [8, Sect. 6, Lemma 4]. It suffices to show $|\ker(\beta_n)| \leqslant p^r$ for all $n \geqslant m_0$. We have

$$\ker(\beta_n) = \{I_{n,\chi} \in \mathfrak{J}_n \mid I_{n,\chi} = Z_n u_\chi \text{ for some } u_\chi \in A_n\}.$$

Let $p^{l(\chi)}$, with $0 \leqslant l(\chi) \leqslant n$, be the order of $\chi \in \hat{G}_n$. If $I_{n,\chi} = Z_n u_\chi$ for some $u_\chi \in A_n$ then setting $a_\chi = u_\chi^{p^{l(\chi)}}$ we have $\sigma(a_\chi) = (\chi(\sigma)u_\chi)^{p^{l(\chi)}} = a_\chi$, for all $\sigma \in G_n$, hence $a_\chi \in Z_n$. Since $I_{n,\chi}^{p^{l(\chi)}} = Z_n = Z_n a_\chi$ we get $a_\chi \in Z_n^*$, and $K_n(u_\chi)$ is a cyclic extension of K_n of degree $p^{l(\chi)}$. Setting $\alpha_\chi = a_\chi \bar{a}_\chi^{-1}$ we obtain

$$\alpha_\chi \in Z_n, \qquad \alpha_\chi \alpha_{\bar{\chi}} = 1, \qquad K_n(u_\chi) = K_n(v_\chi) \qquad \text{with} \quad v_\chi^{p^{l(\chi)}} = \alpha_\chi, \quad (\dagger\dagger)$$

since u_χ and $\bar{u}_\chi^{-1}$ both generate $I_{n,\chi}$ because of $\overline{I_{n,\chi}} = I_{n,\chi}^{-1}$.

Choose a sequence $u_\chi \in A_n$, $\chi \in G_n$, such that $\ker(\beta_n) = \{Z_n u_\chi\}$. Let L_n''

be the compositum in D_n of the fields $K_n(u_\chi)$, and let H_n be the Galois group of L_n'' over K_n. Then $\oplus_\chi K_n \cdot u_\chi \subset L_n''$ [2, Cor. 2], hence

$$|\ker(\beta_n)| = \dim_{K_n}\left(\bigoplus_\chi K_n \cdot u_\chi\right) \leqslant \dim_{K_n}(L_n'') = |H_n|.$$

Since L_n'' is unramified over K_n and since K_∞ is totally ramified at all primes of K_n lying above $p\mathbb{Z}$, we have $\dim_{K_\infty}(K_\infty L_n'') = |H_n|$ for all $n \geqslant m_0$. By construction, the field $K_\infty L_n''$ lies in the maximal abelian unramified p-extension of K_∞ in which every prime of K_∞ lying above $p\mathbb{Z}$ is completely decomposed. Now it follows from (††) and [8, Lemma 26] that there is $r \in \mathbb{N}$, r independent of n, such that $|H_n| \leqslant p^r$ for all n. ∎

We define for each $i \in \mathbb{Z}$ an R-algebra homomorphism

$$\hat{v}_i \colon R[\Gamma_n] \to R[\Gamma_n] \qquad \text{via } \hat{v}_i(\tau_n) = \tau_n^i.$$

4.9. LEMMA. *If $A \in \mathrm{Pic}(R[\Gamma_n])$ is in the image of $\alpha \colon H^1(R, \Gamma_n) \to \mathrm{Pic}(R[\Gamma_n])$, then $\hat{v}_i^*(A) = A^i$ for all $i > 0$.*

Proof. Consider the three homomorphisms ε_1, ε_2, and Δ from $R[\Gamma_n]$ to $R[\Gamma_n \times \Gamma_n]$ defined by $\varepsilon_1(\tau_n) = (1, \tau_n)$, $\varepsilon_2(\tau_n) = (\tau_n, 1)$, and $\Delta(\tau_n) = (\tau_n, \tau_n)$. Then $\varepsilon_1^*(A) \cdot \varepsilon_2^*(A) = \Delta^*(A)$ since A is in the image of α [3, Corollary 1.3].

Consider homomorphisms f_i from $R[\Gamma_n \times \Gamma_n]$ to $R[\Gamma_n]$ defined by $f_i(\tau_n^k, \tau_n^l) = \tau_n^{k+il}$ for $i > 0$. We then have $f_i^*(\varepsilon_1^*(A)\varepsilon_2^*(A)) = f_i^*(\varepsilon_1^*(A)) f_i^*(\varepsilon_2^*(A)) = f_i^*(\Delta^*(A))$ and $\hat{v}_i^*(A)A = \hat{v}_{i+1}^*(A)$ for all $i > 0$. This implies $A^2 = \hat{v}_2^*(A)$ when $i = 1$. If $A^i = \hat{v}_i^*(A)$ for $i \geqslant 1$ then $A^{i+1} = \hat{v}_i^*(A)A = \hat{v}_{i+1}^*(A)$. ∎

We are now ready for the proof of Theorem 4.4:

4.4. THEOREM. *Let $R_\infty = \bigcup_n R_n$ be a Γ-extension of R. If $R_n \cdot \bar{R}_n$ has a normal basis over R for all n there is $s \geqslant 0$, independent of n, such that $R_n^{p^s}$ has a normal basis over R for all n.*

Proof. Write A_n (resp. $\bar{A}_n$) for the images of R_n (resp. $\bar{R}_n$) in $\mathrm{Pic}(R[\Gamma_n])$. We then have $A_n \bar{A}_n = 1$ for all n by assumption.

Let μ_{p^k} be the group of p^kth roots of unity in a fixed separable closure K^{sep} of K, and let n_0 be maximal such that $\mu_{p^{n_0}}$ lies in $K(\mu_p)$. Each connected component of $R[\Gamma_n]$ is isomorphic to $R(\mu_{p^k})$ for some k with $0 \leqslant k \leqslant n$. Hence there is $k \geqslant 0$ and a homomorphism

$$\psi_{k,n} \colon R[\Gamma_n] \to R(\mu_{p^k})$$

inducing a homomorphism $\psi_{k,n}^* \colon \mathrm{Pic}(R[\Gamma_n]) \to \mathrm{Pic}(R(\mu_{p^k}))$ such that $I_{k,n} := \psi_{k,n}^*(A_n)$ has the same order as A_n.

Complex conjugation ι induces a homomorphism

$$\iota^*: \mathrm{Pic}(R(\mu_{p^k})) \to \mathrm{Pic}(R(\mu_{p^k})), \qquad [M] \mapsto [\bar{M}] =: \overline{[M]}.$$

We now show $I_{k,n} = \bar{I}_{k,n}$. Let ζ_k be a primitive p^kth root of unity. There is i such that $\psi_{k,n}(\tau_n) = \zeta_k^i$. For $x = \Sigma_j a_j \tau_n^{-j} \in R[\Gamma_n]$ we have

$$\overline{\psi_{k,n}(x)} = \overline{\sum_j a_j \zeta_k^{-ij}} = \sum_j \bar{a}_j \zeta_k^{ij} = \psi_{k,n}(\hat{v}_{-1}(\bar{x})) = \psi_{k,n}(\hat{v}_{p^n-1}(\bar{x})).$$

This implies, using Lemma 4.9 and the equation $A_n \bar{A}_n = 1$,

$$\bar{I}_{k,n} = \overline{\psi^*_{k,n}(A_n)} = \psi^*_{k,n}(\hat{v}^*_{p^n-1}(\bar{A}_n)) = \psi^*_{k,n}(\bar{A}_n^{p^n-1}) = \psi^*_{k,n}(\bar{A}_n^{-1}) = I_{k,n}.$$

Define $\rho: R(\mu_{p^k}) \to R(\mu_{p^k})$ such that

$$\rho(\zeta_k) = \zeta_k^{p^{n_0}+1}.$$

Then $(\rho \circ \psi_{k,n})(x) = \rho(\sum_j a_j \zeta_k^{-ij}) = \sum_j a_j \zeta_k^{-ij(p^{n_0}+1)} = \psi_{k,n}(v_{p^{n_0}+1}(x))$, hence $\rho^*(I_{k,n}) = \rho^*(\psi^*_{k,n}(A_n)) = (\rho \circ \psi_{k,n})^*(A_n) = \psi^*_{k,n}(A_n^{p^{n_0}+1}) = I_{k,n}^{p^{n_0}+1}$ by 4.9. By Proposition 4.8 there is $s \geqslant 0$, independent of n and k, with $I_{k,n}^{p^s} = 1$. Since A_n has the same order as $I_{k,n}$ we have $A_n^{p^s} = 1$. Therefore $R_n^{p^s}$ has a normal basis over R for all n. ∎

ACKNOWLEDGMENT

We express our thanks to the referee for some valuable improvements.

REFERENCES

1. S. U. CHASE, D. K. HARRISON, AND A. ROSENBERG, Galois theory and Galois cohomology of commutative rings, *Mem. Amer. Math. Soc.* **52** (1965), 15–33.
2. L. CHILDS, Abelian Galois extensions of rings containing roots of unity, *Illinois J. Math.* **15** (1971), 273–279.
3. L. CHILDS, The group of unramified Kummer extensions of prime degree, *Proc. London Math. Soc.* **XXXV** (1977), 407–422.
4. G. GARFINKEL AND M. ORZECH, Galois extensions as modules over the group ring, *Canad. J. Math.* **22** (1970), 242–248.
5. C. GREITHER, On Galois extensions of commutative rings with Galois group $\mathbb{Z}/p^n\mathbb{Z}$, preprint.
6. A. GROTHENDIECK, Site et topos étale d'un schema, SGA 4, Exposé VII, *Springer Lecture Notes Math.* **270** (1972), 341–365.
7. D. K. HARRISON, Abelian extensions of commutative rings, *Mem. Amer. Math. Soc.* **52** (1965), 1–14.
8. K. IWASAWA, On $\mathbb{Z}_l$-extensions of algebraic number fields, *Ann. of Math.* **98** (1973), 246–326.

9. I. KERSTEN AND J. MICHALIČEK, Das Einbettungsproblem für zyklische p^n-Erweiterungen über einem semilokalen Ring, *J. Algebra* **82** (1983), 275–281 .
10. I. KERSTEN AND J. MICHALIČEK, Kummer theory without roots of unity, *J. Pure Appl. Algebra* **50** (1988), 21–72.
11. I. KERSTEN AND J. MICHALIČEK, On Γ-extensions of totally real and complex multiplication fields, *C.R. Math. Rep. Acad. Sci. Canad.* **IX** (1987).
12. S. LANG, "Cyclotomic fields, II," Springer-Verlag, New York/Heidelberg/Berlin, 1980.
13. H. W. LENSTRA, A normal basis theorem for infinite Galois extensions, *Indag. Math.* **47** (1985), 221–228.
14. M. ORZECH, A cohomological description of abelian Galois extensions, *Trans. Amer. Math. Soc.* **137** (1969), 481–499.
15. L. C. WASHINGTON, "Introduction to Cyclotomic Fields," Springer-Verlag, New York/ Heidelberg/Berlin, 1982.